Separability of Density Matrices and Conditional Information Transmission

Robert R. Tucci
P.O. Box 226
Bedford, MA 01730
tucci@ar-tiste.com

February 1, 2008

Abstract

We give necessary and sufficient conditions under which a density matrix acting on a two-fold tensor product space is separable. Our conditions are given in terms of quantum conditional information transmission.

Ref.[1] proposed using quantum conditional information transmission as a measure of entanglement. In its simplest case, this measure requires one speaker and two listeners. On the other hand, the simplest case of separability of density matrices is defined for two listeners but no speaker. Thus, it is not immediately apparent how quantum conditional information transmission is related to separability. And yet, they must be closely related since they are both closely related to the phenomenon of quantum entanglement. In this paper, we present a theorem that elucidates the hidden relationship between conditional information transmission and separability. The theorem gives necessary and sufficient conditions for the separability of density matrices acting on a two-fold tensor product space. The theorem can be easily generalized to the case of n-fold tensor products.

We will use $\mathcal{H}_{\underline{a}}, \mathcal{H}_{\underline{b}}, \ldots$ to represent Hilbert spaces (finite dimensional ones for simplicity), and $\mathcal{H}_{\underline{a},\underline{b}}$ to represent $\mathcal{H}_{\underline{a}} \otimes \mathcal{H}_{\underline{b}}$, the tensor product of $\mathcal{H}_{\underline{a}}$ and $\mathcal{H}_{\underline{b}}$. $dim(\mathcal{H})$ will stand for the dimension of the Hilbert space $\mathcal{H}$. The set of all density matrices acting on a Hilbert space $\mathcal{H}$ will be denoted by $\mathcal{D}(\mathcal{H})$. If $\rho_{\underline{xy}} \in \mathcal{D}(\mathcal{H}_{\underline{xy}})$, we will denote the partial traces of $\rho_{\underline{xy}}$ by $\rho_{\underline{x}} = \mathrm{tr}_{\underline{y}} \rho_{\underline{xy}}$ and $\rho_{\underline{y}} = \mathrm{tr}_{\underline{x}} \rho_{\underline{xy}}$. For any set S, we will use $|S|$ to represent the number of elements in S.

We will say $\rho \in \mathcal{D}(\mathcal{H}_{\underline{xy}})$ is *separable* (or more precisely, $\underline{x}, \underline{y}$ *separable*) if ρ can be expressed as

$$\rho = \sum_e w_e \rho^e_{\underline{x}} \rho^e_{\underline{y}} \ , \tag{1}$$

where the w_e, called *weights*, are non-negative numbers that sum to 1, and where for all e, $\rho^e_{\underline{x}} \in \mathcal{D}(\mathcal{H}_{\underline{x}})$ and $\rho^e_{\underline{y}} \in \mathcal{D}(\mathcal{H}_{\underline{y}})$. *Non-entangled* $\underline{x}, \underline{y}$ states are usually defined as those which are $\underline{x}, \underline{y}$ separable.

We will say $\rho \in \mathcal{D}(\mathcal{H}_{\underline{xye}})$ is *conditionally separable* (or more precisely, $\underline{x}, \underline{y} | \underline{e}$ *separable*) if ρ can be expressed as

$$\rho = \sum_e w_e |e\rangle\langle e| \rho^e_{\underline{x}} \rho^e_{\underline{y}} \ , \tag{2}$$

where the w_e, called *weights*, are non-negative numbers that sum to 1, the states $|e\rangle$ are an orthonormal basis for $\mathcal{H}_{\underline{e}}$, and for all e, $\rho^e_{\underline{x}} \in \mathcal{D}(\mathcal{H}_{\underline{x}})$ and $\rho^e_{\underline{y}} \in \mathcal{D}(\mathcal{H}_{\underline{y}})$.

Suppose A is a set of random variables. For example, $A = \{\underline{a}, \underline{b}\}$. If $\rho \in \mathcal{D}(\mathcal{H}_A)$ and $A' \subset A$, then we will use $S_\rho(A')$ to represent $S(\mathrm{tr}_{A-A'} \rho)$, where $S(\cdot)$ is the von Neumann entropy. For example, if $\rho \in \mathcal{D}(\mathcal{H}_{\underline{a},\underline{b}})$, then $S_\rho(\underline{a}) = S(\mathrm{tr}_{\underline{b}} \rho)$. If $\rho \in \mathcal{D}(\mathcal{H}_{\underline{xye}})$, we define the quantum *conditional mutual information*, or *conditional information transmission* by

$$S_\rho[(\underline{x} : \underline{y}) | \underline{e}] = S_\rho(\underline{x}, \underline{e}) + S_\rho(\underline{y}, \underline{e}) - S_\rho(\underline{x}, \underline{y}, \underline{e}) - S_\rho(\underline{e}) \ . \tag{3}$$

The classical counterpart of this is the classical conditional mutual information, which is defined, for random variables $\underline{x}, \underline{y}, \underline{e}$ with a joint distribution $P(x, y, e)$, by

$$H[(\underline{x}:\underline{y})|\underline{e}] = \sum_{x,y,e} P(x,y,e) \log_2 \frac{P(x,y|e)}{P(x|e)P(y|e)} \ . \tag{4}$$

See Ref.[2] for a review of classical and quantum entropy presented in the same notation used in this paper.

For any $\rho \in \mathcal{D}(\mathcal{H}_{\underline{x}\underline{y}\underline{e}})$,

$$S_\rho[(\underline{x}:\underline{y})|\underline{e}] \geq 0 \ . \tag{5}$$

This is called the *strong subadditivity inequality* for quantum entropy. It was first proven by Lieb-Ruskai in Ref.[3]. More recently, it has been shown[4] that the strong subadditivity inequality becomes an equality (i.e., "is saturated") if and only if ρ satisfies

$$\log \rho = \log \rho_{\underline{x}\underline{e}} + \log \rho_{\underline{y}\underline{e}} - \log \rho_{\underline{e}} \ . \tag{6}$$

Classical random variables $\underline{x}, \underline{y}, \underline{e}$ with joint distribution $P(x,y,e)$ satisfy

$$H[(\underline{x}:\underline{y})|\underline{e}] \geq 0 \ , \tag{7}$$

which is the classical counterpart of Eq.(5). This inequality is saturated if and only if

$$P(x,y|e) = P(x|e)P(y|e) \tag{8}$$

for all x, y, e. When Eq.(8) is true, we say $\underline{x}, \underline{y}$ are *conditionally independent*. Taking the logarithm of both sides of Eq.(8) yields

$$\log P(x,y,e) = \log P(x,e) + \log P(y,e) - \log P(e) \ , \tag{9}$$

which is the classical counterpart of Eq.(6).

Theorem 1: $\rho \in \mathcal{D}(\mathcal{H}_{\underline{x}\underline{y}})$ is $\underline{x}, \underline{y}$ separable if and only if there exists a Hilbert space $\mathcal{H}_{\underline{e}}$ and a density matrix $\sigma \in \mathcal{D}(\mathcal{H}_{\underline{x}\underline{y}\underline{e}})$ such that

1. $\rho = \mathrm{tr}_{\underline{e}} \sigma$,
2. $S_\sigma[(\underline{x}:\underline{y})|\underline{e}] = 0$,
3. $\sigma_{\underline{y}\underline{e}}, \sigma_{\underline{x}\underline{e}}$ and $\sigma_{\underline{e}}$ commute pairwise,
4. the eigenvalues of $\sigma_{\underline{e}}$ are are non-zero and non-degenerate.

proof:

($\Rightarrow$) ρ can be expanded as in Eq.(1). We can always choose the weights w_e of the expansion to be non-zero and non-degenerate. Indeed, if $w_e = 0$, we just eliminate that term from the expansion. If $e_1 \neq e_2$ and $w_{e_1} = w_{e_2}$, then we replace the e_1 and e_2 terms of the expansion by

$$
\begin{aligned}
& w_{e_1}(\rho_{\underline{x}}^{e_1}\rho_{\underline{y}}^{e_1} + \rho_{\underline{x}}^{e_2}\rho_{\underline{y}}^{e_2}) = \\
& \quad = w_{e_1}\rho_{\underline{x}}^{e_1}\rho_{\underline{y}}^{e_1} + (\frac{w_{e_1}}{2} + \epsilon)\rho_{\underline{x}}^{e_2}\rho_{\underline{y}}^{e_2} + (\frac{w_{e_1}}{2} - \epsilon)\rho_{\underline{x}}^{e_2}\rho_{\underline{y}}^{e_2} = \\
& \quad = \sum_{j=1}^{3} w'_{e_j}\rho_{\underline{x}}^{\prime e_j}\rho_{\underline{y}}^{\prime e_j} \ , \qquad (10)
\end{aligned}
$$

where we have define a new e value called e_3 and we have set $w'_{e_1} = w_{e_1}$, $w'_{e_2} = \frac{w_{e_1}}{2} + \epsilon$ and $w'_{e_3} = \frac{w_{e_1}}{2} - \epsilon$. For small enough $\epsilon > 0$, we achieve our goal of representing ρ as in Eq.(1) with weights that are non-degenerate and non-zero. If E is the new set of e values, let $\mathcal{H}_{\underline{e}}$ be a Hilbert space of dimension $|E|$, and let $|e\rangle$ for $e \in E$ be an orthonormal basis for $\mathcal{H}_{\underline{e}}$. Define $\sigma \in \mathcal{D}(\mathcal{H}_{\underline{xye}})$ by

$$
\sigma = \sum_{e \in E} w_e |e\rangle\langle e| \rho_{\underline{x}}^{e}\rho_{\underline{y}}^{e} \ . \qquad (11)
$$

Thus, σ is $\underline{x}, \underline{y}|\underline{e}$ separable. Clearly, $\rho = \mathrm{tr}_{\underline{e}}\sigma$. In Ref.[1], it is shown by straightforward computation that any $\underline{x}, \underline{y}|\underline{e}$ separable density matrix σ satisfies $S_\sigma[(\underline{x} : \underline{y})|\underline{e}] = 0$. σ has the following partial traces:

$$
\sigma_{\underline{e}} = \sum_e w_e |e\rangle\langle e| \ , \qquad (12)
$$

$$
\sigma_{\underline{xe}} = \sum_e w_e |e\rangle\langle e| \rho_{\underline{x}}^{e} \ , \qquad (13)
$$

$$
\sigma_{\underline{ye}} = \sum_e w_e |e\rangle\langle e| \rho_{\underline{y}}^{e} \ . \qquad (14)
$$

Clearly, $\sigma_{\underline{ye}}, \sigma_{\underline{xe}}$ and $\sigma_{\underline{e}}$ commute pairwise. The eigenvalues of $\sigma_{\underline{e}}$ are the w_e, which are non-zero and non-degenerate.

($\Leftarrow$) $S_\sigma[(\underline{x} : \underline{y})|\underline{e}] = 0$ so Eq.(6) is true for σ. In fact, since $\sigma_{\underline{ye}}, \sigma_{\underline{xe}}$ and $\sigma_{\underline{e}}$ commute pairwise, and $\rho_{\underline{e}}$ has non-zero eigenvalues, we can combine the logarithms to obtain

$$
\sigma = \sigma_{\underline{ye}}\sigma_{\underline{xe}}(\sigma_{\underline{e}})^{-1} \ . \qquad (15)
$$

Since $\sigma_{\underline{e}}$ is a Hermitian matrix, it can be diagonalized:

$$
\sigma_{\underline{e}} = \sum_e w_e |e\rangle\langle e| \ , \qquad (16)
$$

where w_e and $|e\rangle$ for all e are the eigenvalues and eigenvectors of $\sigma_{\underline{e}}$. One has that

$$
\sigma_{\underline{e}}\sigma_{\underline{xe}} = \sigma_{\underline{xe}}\sigma_{\underline{e}} \ . \qquad (17)
$$

Thus,

$$w_e\langle e|\sigma_{\underline{xe}}|e'\rangle = \langle e|\sigma_{\underline{xe}}|e'\rangle w_{e'} \tag{18}$$

for all e, e'. Since the eigenvalues w_e of $\sigma_{\underline{e}}$ are non-degenerate, $e \neq e'$ implies $w_e \neq w_{e'}$, and therefore $\langle e|\sigma_{\underline{xe}}|e'\rangle = 0$. It follows that $\sigma_{\underline{xe}}$ is diagonal in its $\mathcal{H}_{\underline{e}}$ sector:

$$\sigma_{\underline{xe}} = \sum_{x,x',e} A^e_{x,x'}|e,x\rangle\langle e,x'| \ , \tag{19}$$

where for all x, x', e, $A^e_{x,x'}$ is a complex number, and where $|x\rangle$ for all x is any orthonormal basis of $\mathcal{H}_{\underline{x}}$. If for each e, $\rho^e_{\underline{x}} \in \mathcal{D}(\mathcal{H}_{\underline{x}})$ is defined by

$$\rho^e_{\underline{x}} = \sum_{x,x'} \frac{A^e_{x,x'}}{w_e}|x\rangle\langle x'| \ , \tag{20}$$

then Eq.(19) can be rewritten as

$$\sigma_{\underline{xe}} = \sum_e w_e|e\rangle\langle e|\rho^e_{\underline{x}} \ . \tag{21}$$

By a similar argument, $\sigma_{\underline{ye}}$ is also diagonal in its $\mathcal{H}_{\underline{e}}$ sector and can be expressed as

$$\sigma_{\underline{ye}} = \sum_e w_e|e\rangle\langle e|\rho^e_{\underline{y}} \ , \tag{22}$$

where for all e, $\rho^e_{\underline{y}} \in \mathcal{D}(\mathcal{H}_{\underline{y}})$. Our newly found, diagonal in the $\mathcal{H}_{\underline{e}}$ sector, expressions for $\sigma_{\underline{ye}}, \sigma_{\underline{xe}}$ and $\sigma_{\underline{e}}$ can now be substituted into Eq.(15) to get

$$\sigma = \sum_e w_e|e\rangle\langle e|\rho^e_{\underline{x}}\rho^e_{\underline{y}} \ . \tag{23}$$

Thus, σ is $\underline{x}, \underline{y}|\underline{e}$ separable. Taking the $\underline{e}$ trace of this σ to get ρ, we see that ρ is $\underline{x}, \underline{y}$ separable. QED

There probably exist certain $\rho \in \mathcal{D}(\mathcal{H}_{\underline{xy}})$ for which conditions 1 to 4 on the right hand side of Theorem 1 cannot be achieved for finite $dim(\mathcal{H}_{\underline{e}})$, but can be achieved in the limit $dim(\mathcal{H}_{\underline{e}}) \rightarrow \infty$. Such ρ could be described as being weakly separable.

Let $\mathcal{D}_{insep}(\mathcal{H}_{\underline{xy}})$ be the set of all $\rho \in \mathcal{D}(\mathcal{H}_{\underline{xy}})$ which are not $\underline{x}, \underline{y}$ separable. Let $\mathcal{D}_{pos}(\mathcal{H}_{\underline{xy}})$ be the set of all $\rho \in \mathcal{D}(\mathcal{H}_{\underline{xy}})$ for which all extensions $\sigma \in \mathcal{D}(\mathcal{H}_{\underline{xye}})$ such that $\rho = \mathrm{tr}_{\underline{e}}\sigma$ satisfy $S_\sigma[(\underline{x} : \underline{y})|\underline{e}] \neq 0$. Then, by Theorem 1, $\mathcal{D}_{pos}(\mathcal{H}_{\underline{xy}}) \subset \mathcal{D}_{insep}(\mathcal{H}_{\underline{xy}})$. Density matrices in $\mathcal{D}_{pos}(\mathcal{H}_{\underline{xy}})$ and those in $\mathcal{D}_{insep}(\mathcal{H}_{\underline{xy}}) - \mathcal{D}_{pos}(\mathcal{H}_{\underline{xy}})$ exhibit different kinds of entanglement.

Some goals for future research are: give concrete examples of Theorem 1; explore the connection between Theorem 1 and the necessary condition for separability given by Peres[5], and the bound entanglement discovered by Horodecki.[6].

Acknowledgements: I thank M.A. Nielsen, D. Petz and M.B Ruskai for their generosity in communicating to me that the quantum strong subadditivity inequality is saturated iff Eq.(6).

References

[1] R.R. Tucci, "Quantum Entanglement and Conditional Information Transmission", Los Alamos eprint quant-ph/9909040 .

[2] R.R. Tucci, "Quantum Information Theory - A Quantum Bayesian Nets Perspective", Los Alamos eprint quant-ph/9909039 .

[3] E. Lieb, M.B. Ruskai, J. of Math. Phys. **14**, 1938 (1973).

[4] This result was communicated to the author by M.B. Ruskai and M.A. Nielsen, who intend to publish their own proof in the near future. The result was also independently communicated to the author by D. Petz, who pointed out that strong subadditivity follows from monotonicity, so this result is a corollary of his paper: Commun. Math Phys. **105**, 123 (1986). See also pages 23-24 of M. Ohya, D. Petz, *Quantum Entropy and Its Use* (Springer-Verlag, Heidelberg, 1993).

[5] A. Peres, Phys. Rev. Lett. A **76**, 1413 (1997). Also available as Los Alamos eprint quant-ph/9604005 .

[6] P. Horodecki, Phys. Rev. Lett. A **232**, 333 (1997). Also available as Los Alamos eprint quant-ph/9703004 .